



Information Management, Technology & Reengineering and Joint Medical Information Systems Managers' Internal Control Program



INFORMATION BULLETIN

Volume 4, Issue 3

June 26, 2007

Special Message:

The Fiscal Year 2007 IMT&R/JMIS Annual Statement of Assurance was submitted on June 6, 2007. A special thanks to all AU Managers and MIC Program Representatives for all their hard work and support in putting together this report.



"The central theme of internal control is to identify risks to the achievement of an organization's objectives and to do what is necessary to manage those risks."

Protecting Government Assets

Contractors generally furnish the property/equipment necessary to perform government contracts. However, if contractors possess government property, the government requires them to be responsible, accountable, and to maintain the official records for all Government-Furnished Property (GFP).

GFP is defined by the Federal Acquisition Regulations (FAR), Subpart 45.1 as **"property in the possession of, or directly acquired by, the Government and subsequently made available to the contractor."** Contractors who possess GFP are required to create a property control system for the government property which should be in writing and contain a procedure to locate any property within a reasonable period of time.



The Property Administrators, generally the Contracting Officer's Representative (COR) for TMA contracts, are responsible for ensuring that the contractor's property control system is compliant with the government property clauses in the contract.

TMA's property clause requires all contractors to maintain a detailed inventory accounting system for GFP and Contractor-acquired-Government Owned property (CAP). The inventory accounting system must specify, as a minimum: product description (make, model), government tag number, date of receipt, name of recipient, location of receipt, current location, purchase cost (if CAP), and contract/order number under which the



equipment is being used. (Source: [D/SIDDOMS 3 Request for Proposal \(RFP\)/Task Order Template](#))

Contractors must also perform periodic physical inventories of all GFP/CAP. The regularity and method of inventory is determined by the contractor, but subject to the approval of the property administrator. The TMA Task Order Template requires contractors to either: a) attach an updated inventory report to each Monthly Progress Report, or b) certify that the inventory report has been updated and is available for Government review. In either case the Contractor's inventory listing must be available for Government review within one business day of COR request.

CIO Assessment for Title 40 Oversight

On April 2, 2007, the DoD CIO implemented a risk-based approach for oversight of Title 40/Clinger Cohen Act (CCA) requirements for Major Automated Information System (MAIS) programs. This new policy is aimed at decentralizing oversight, maximizing up-

front involvement in the IT investment process, and alleviating redundancies. Under this risk-based oversight process, the DoD CIO may defer to Component CIOs, oversight of Title 40/CCA for MAIS programs. Component CIOs



must complete a Capability Assessment which will be used by the DoD CIO to determine the Component's oversight capability and the program risk.

In conjunction with the self-assessment, internal

Continued on page 2

CIO Assessment for Title 40 Oversight Cont'd

controls must be established, monitored, and reported against to ensure IT investments are acquired and maintained with respect to the Component's strategic and information resource management goals.

Internal controls will be evaluated to

determine sufficiency, effectiveness, and applicability to support the CIO's Title 40 responsibilities.

Deficiencies identified during the self-assessment should be considered in the CIO's continuous process improvement program.

To view this policy, visit the Federal and DoD Policy/Guidance page of the MHS CIO Website located at <http://www.ha.osd.mil/mhscio/policy-guid.htm>.

Don't Become a Victim of Personal Identity Theft

Identity theft and identity fraud are terms used to refer to crimes in which someone wrongfully obtains and uses another person's personal data in some way that involves fraud or deception, usually for monetary gain.

There are two types of identity theft, "account takeover" and application fraud (AKA "true name fraud"). Account takeover occurs when a thief steals your *existing* credit card information and purchases goods and/or services using the actual credit card or the credit card number and expiration date. Application fraud occurs when a thief uses a social security number (SSN) and other identifying information to open *new* accounts in the victim's name.

Stealing wallets used to be the most common way identity thieves obtained personal data, but now thieves use a variety of methods to obtain this valuable information. Some of the more common methods include: dumpster diving for credit card applications and other documentation containing SSNs; accessing credit reports fraudulently by posing as an employer, loan officer, or landlord; stealing names and SSNs from personnel files in the workplace; "shoulder surfing" at ATMs to capture pin numbers; public record sites on the internet; and "phishing" or sending fake emails asking for account information and passwords. So what can we do to reduce the risk

of becoming a victim of identity theft or fraud? The US Department of Justice says just remember the word "**SCAM**".



S – be **stingy** about giving out your personal information (SSNs, credit card numbers) to others unless you trust them.

C – **Check** your financial records frequently.

A – **Ask** for copies of your credit reports about every four months.

M – Safely **maintain** copies of your financial records.

Awareness is your best defense against identity theft.

Source: <http://www.usdoj.gov/criminal/fraud/websites/idtheft.html>

High-Tech ID Cards for Federal Employees & Contractors

On August 27, 2004, the President signed the [Homeland Security Presidential Directive 12](#) (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and Contractors." The objective of the HSPD-12 is to enhance security, increase government efficiency, reduce identity fraud, and protect personal privacy by implementing a **government-wide standard** for **secure** and **reliable** forms of identification for employees and contractors.

The terms "secure and reliable", according to this directive, refer to identification that: (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly

resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

By October 2008 all federal employees and contractors should be issued new identification cards allowing them access to multiple federal buildings and information systems. The new cards, referred to as Personal Identity Verification (PIV) cards, will have "smart" features including Public Key Infrastructure and biometrics. They will contain a printed picture and a

computer chip containing fingerprints, a personal identification number, and access information such as clearance levels and codes to access federal buildings and information systems.



When issuing the cards, organizations must use an approved identity proofing and registration process. This includes: background checks utilizing sources like the National Agency Check with written inquiries; FBI fingerprint checks; two forms of identification for applicants; and adequate separation of duties, meaning that no one person can request, authorize, and issue a badge.

MILCOM Employee Sentenced for Accepting Kickbacks

The DoD Office of the Inspector General (IG) announced that a former MILCOM Systems Corporation employee, Reginald Wayne Page, was sentenced in a Virginia District Court for accepting kickbacks in violation of the Anti-Kickback Act.

As a Division Purchasing Manager for MILCOM, Page approved the award

of all freight transportation contracts. During their investigation, the DoD IG found that Page had accepted over 125 items of value from Air Cargo, over a 5 year period, in return for the award of transportation contracts.

These items, totaling approximately \$7,400, included lunches, dinners, con-

cert tickets, various travel expenses, lodging, football tickets and more.



Page was sentenced to 8 months incarceration, 120 days of home confinement, 3 years supervised probation, and a \$100 special assessment.

Assessable Unit Managers' Corner

The subject of internal control has been included in almost every GAO and IG Audit over the past several years. In an effort to better understand the need for and importance of internal controls let's review some of the key areas auditors focus on during reviews:

Segregation of Duties: Duties/functions should be separated so that one person does not perform the process from beginning to end.

Safeguarding Assets: Ensure protec-

tive measures are in place to properly and securely maintain assets.

Review and Approval: When a process is performed within an organization, there should always be another level of review and approval performed by a knowledgeable individual independent of the process.

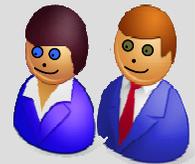
Policies and Procedures: Written policies and procedures should codify management's criteria for executing an organization's operations.

Efficiency and Effectiveness: Utilize efficient and effective performance to

ensure that goals and objectives are accurately accomplished in a timely fashion, while using minimal resources.

Timeliness: Ensure established suspenses/deadlines are met.

AU Managers should pay close attention to the importance of these areas during risk assessments and internal control reviews.



Audit Reviews Highlight Internal Control

During their review of DoD Compliance with Federal Managers' Financial Integrity Act of 1982, the DoD IG determined that the DoD and Military Departments' **Annual Statements of Assurance (ASAs)** were not always complete and that they **may contain inaccurate information**. This was due, in part, because DoD: 1) didn't fully consider all of the auditor-identified and DoD-acknowledged weaknesses when reporting material weaknesses; 2) provided a level of assurance on internal control over financial reporting that was inconsistent with known DoD material weaknesses; and 3) **reported targeted correction dates for system weaknesses that weren't supported by the Component's ASA**. To read more about this report (IG D-2007-093) please visit http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm.

In support of their legislative mandate to review DoD's Business Systems Modernization, the GAO assessed whether the department's corporate investment management approach complies with relevant Federal Guidance. During this review, the GAO found that while the DoD has established the management structures required to effectively manage its business system investments, they still **lack the defined policies and procedures** that the GAO's IT Investment Management Framework defines. Specifically, DoD has not fully documented business system investment policies and procedures related to five of the nine key project-level management practices. DoD also doesn't have policies and procedures in place for: defining the portfolio criteria; creating and evaluating the portfolio; and conducting post implementation reviews for all business systems. To read more about this report (GAO-07-538) and the DoD's response please visit http://www.ha.osd.mil/mhscio/Man_Ctrl_Prog_Audits.htm.



"Internal control provides the opportunity to improve the understanding of your organization, leading to better support and fewer problems."